

Quantum exam

Nguyen Ba An*

*School of Computational Sciences, Korea Institute for Advanced Study,
207-43 Cheongryangni 2-dong, Dongdaemun-gu, Seoul 130-722, Republic of Korea*

Absolutely and asymptotically secure protocols for organizing an exam in a quantum way are proposed basing judiciously on multipartite entanglement. The protocols are shown to stand against common types of eavesdropping attack.

PACS numbers: 03.67.Hk, 03.65.Ud, 03.67.Dd

1. Introduction

Simultaneous distance-independent correlation between different systems called entanglement [1] is the most characteristic trait that sharply distinguishes between quantum and classical worlds. At present entanglement between two systems, i.e. bipartite entanglement, is quite well understood, but that between more than two systems, i.e. multipartite entanglement, remains still far from being satisfactorily known. In spite of that, multipartite entanglement has proven to play a superior role in recently emerging fields of quantum information processing and quantum computing since it exhibits a much richer structure than bipartite entanglement. Motivation for studying multipartite entanglement arises from many reasons some of which are listed now. First, multipartite entanglement provides a unique means to check the Einstein locality without invoking statistical arguments [2], contrary to the case of Bell inequalities using bipartite entanglement. Second, multipartite entanglement serves as a key ingredient for quantum computing to achieve an exponential speedup over classical computation [3]. Third, multipartite entanglement is central to quantum error correction [4] where it is used to encode states, to detect errors and, eventually, to allow fault-tolerant quantum computation [5]. Fourth, multipartite entanglement helps to better characterize the critical behavior of different many-body quantum systems giving rise to a unified treatment of the quantum phase transitions [6]. Fifth, multipartite entanglement is crucial also in condensed matter phenomena and might solve some unresolved problems such as high-T superconductivity [7]. Sixth, multipartite entanglement is recognized as a unreplaceable or efficient resource to perform tasks involving a large number of parties such as network teleportation [8], quantum cryptography [9], quantum secret sharing [10], remote entangling [11], quantum (tele)cloning [12], quantum Byzantine agreement [13], etc. Finally, multipartite entanglement is conjectured to yield a wealth of fascinating and unexplored physics [14]. Current research in multipartite entanglement is progressing along two directions in parallel. One direction deals with problems such as how to classify [15], quantify [16], generate/control/distill [17] and witness [18] multipartite entanglement. The other direction proceeds to advance various applications exploiting the nonclassical multiway correlation inherent in multipartite entanglement [8, 9, 10, 11, 12, 13]. Our work here belongs to the second direction mentioned above. Namely, we propose protocols to organize the so-called quantum exam which will be specified in the next section. To meet the necessary confidentiality of the exam we use suitable multipartite GHZ entangled states [2] as the quantum channel. We consider two scenarios. One scenario is absolutely secure provided that the participants share a prior proper multipartite entanglement. The other scenario can be performed directly without any nonlocal quantum arrangements in the past but it is only asymptotically secure. Both the scenarios are shown to stand against commonly utilized eavesdropping attacks.

2. Quantum exam

Exploiting the superdense coding feature possessed in bipartite entanglement we have recently proposed a quantum dialogue scheme [19] (see also [20]) allowing two legitimate parties to securely carry out their conversation. In this work multipartite entanglement will be judiciously exploited to do a more sophisticated task. Suppose that a teacher Alice wishes to organize an important exam with her remotely separate students Bob 1, Bob 2, and Bob N . Alice gives her problem to all Bobs and, after some predetermined period of time, asks each Bob to return a solution independently. Alice's problem should be kept confidential from any outsiders. The solution of a Bob should be accessible only to Alice but not to anyone else including the $N - 1$ remaining Bobs. Such confidentiality constraints cannot be maintained even when Alice and Bobs are connected by authentic classical channels because any classical communication could be eavesdropped perfectly without a track left behind. However, combined with appropriate quantum channels such an exam is accomplishable. We call it quantum exam, i.e. an exam organized in a quantum way to guarantee the required secrecy.

*Electronic address: nbaan@kias.re.kr

Let Alice's problem is a binary string

$$Q = \{q_m\} \quad (1)$$

and the solution of a Bob is another string

$$R_n = \{r_{nm}\} \quad (2)$$

where $n = 1, 2, \dots, N$ labels the Bob while $q_m, r_{nm} \in \{0, 1\}$ with $m = 1, 2, 3, \dots$ denote a secret bit of Alice and a Bob.

2.1. Absolutely secure protocol

An exam consists of two stages. In the first stage Alice gives a problem to Bobs and in the second stage she collects Bobs' solutions.

The problem-giving process

To securely transfer the problem from Alice to Bobs the following steps are to be proceeded.

- a1) Alice and Bobs share beforehand a large number of ordered identical $(N + 1)$ -partite GHZ states in the form

$$|\Psi_m\rangle \equiv |\Psi\rangle_{a_m 1_m \dots N_m} = \frac{1}{\sqrt{2}} (|00\dots 0\rangle_{a_m 1_m \dots N_m} + |11\dots 1\rangle_{a_m 1_m \dots N_m}) \quad (3)$$

of which qubits a_m are with Alice and qubits n_m with Bob n .

- a2) For a given m , Alice measures her qubit a_m in the basis $\mathcal{B}_z = \{|0\rangle, |1\rangle\}$, then asks Bobs to do so with their qubits n_m . All the parties obtain the same outcome j_m^z where $j_m^z = 0$ ($j_m^z = 1$) if they find $|0\rangle$ ($|1\rangle$).
- a3) Alice publicly broadcasts the value $x_m = q_m \oplus j_m^z$ (\oplus denotes an addition mod 2).
- a4) Each Bob decodes Alice's secret bit as $q_m = x_m \oplus j_m^z$.

This problem-giving process is absolutely secure because j_m^z , for each m , takes on the value of either 0 or 1 with an equal probability resulting in a truly random string $\{j_m^z\}$ which Alice uses as a one-time-pad to encode her secret problem $\{q_m\}$ simultaneously for all Bobs who also use $\{j_m^z\}$ to decode Alice's problem.

The solution-collecting process

After a predetermined period of time depending on the problem difficulty level Alice collects the solution from independent Bobs as follows.

- b1) Alice and Bobs share beforehand a large number of ordered nonidentical $(N + 1)$ -partite GHZ states in the form

$$|\Phi_m\rangle \equiv |\Phi\rangle_{a_m 1_m \dots N_m} = U_m |\Psi\rangle_{a_m 1_m \dots N_m} \quad (4)$$

with

$$U_m = I_{a_m} \otimes u(s_{1_m}) \otimes u(s_{2_m}) \otimes \dots \otimes u(s_{N_m}) \quad (5)$$

where I_{a_m} is the identity operator acting on qubit a_m and

$$u(s_{n_m}) = (|0\rangle\langle 1| + |1\rangle\langle 0|)^{s_{n_m}} \quad (6)$$

is a unitary operator acting on qubit n_m . For each n and m , the value of s_{n_m} chosen at random between 0 and 1 is known only to Alice but by no means to any other person including Bobs. Qubits a_m are with Alice and qubits n_m with Bob n .

- b2) For a given m , Alice measures her qubit a_m in \mathcal{B}_z with the outcome $j_{a_m}^z = \{0, 1\}$, then asks Bobs to do so with their qubits n_m with the outcome $j_{n_m}^z = \{0, 1\}$.
- b3) Each Bob n publicly broadcasts the value $y_{nm} = r_{nm} \oplus j_{n_m}^z$.

b4) Alice decodes the solution of Bob n as $r_{nm} = y_{nm} \oplus [\delta_{0,s_{nm}} j_{a_m}^z + \delta_{1,s_{nm}} (j_{a_m}^z \oplus 1)]$.

In the solution-collecting process the outcomes $j_{a_m}^z$ and $j_{n_m}^z$ are not the same anymore in general, but they are dynamically correlated as $j_{n_m}^z = \delta_{0,s_{nm}} j_{a_m}^z + \delta_{1,s_{nm}} (j_{a_m}^z \oplus 1)$. This correlation allows only Alice who knows the value of $\{s_{nm}\}$ to decode the solution of a Bob after she obtains her own measurement outcome $j_{a_m}^z$. As is clear, each of the N strings $\{j_{1_m}^z\}, \{j_{2_m}^z\}, \dots, \{j_{N_m}^z\}$ appears truly random and each such a string is used by a Bob and Alice only one time to encode/decode a secret solution $\{r_{nm}\}$. The above solution-collecting process is therefore absolutely secure as well.

The essential condition to ensure absolute security of the quantum exam is a prior sharing of the entangled states $\{|\Psi_m\rangle\}$ and $\{|\Phi_m\rangle\}$ between the teacher Alice and the students Bobs. It is therefore necessary to propose methods for multipartite entanglement sharing.

The $|\Psi_m\rangle$ -sharing process

Alice and Bobs can securely share the states $\{|\Psi_m\rangle\}$ as follows.

- c1) Alice generates a large enough number of identical states $|\Psi_m\rangle$ defined in Eq. (3) [21]. For each such state she keeps qubit a_m and sends qubits $1_m, 2_m, \dots, N_m$ to Bob 1, Bob 2, ..., Bob N , respectively. Before sending a qubit n_m Alice authenticates Bob n of that action.
- c2) After receiving a qubit each Bob also authenticates Alice independently.
- c3) Alice selects at random a subset $\{|\Psi_l\rangle\}$ out of the shared $|\Psi_m\rangle$ -states and lets Bobs know that subset. For each state of the subset Alice measures her qubit randomly in \mathcal{B}_z or in $\mathcal{B}_x = \{|+\rangle, |-\rangle\}$ with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Then she asks every Bob to measure their qubits in the same basis as hers. Alice's (Bobs') outcome in \mathcal{B}_z is $j_{a_l}^z (j_{n_l}^z) = \{0, 1\}$ corresponding to finding $\{|0\rangle, |1\rangle\}$ and that in \mathcal{B}_x is $j_{a_l}^x (j_{n_l}^x) = \{+1, -1\}$ corresponding to finding $\{|+\rangle, |-\rangle\}$.
- c4) Alice requires each Bob to publicly reveal the outcome of each his measurement and makes an analysis. For those measurements in \mathcal{B}_z she compares $j_{a_l}^z$ with $j_{n_l}^z$: if $j_{a_l}^z = j_{n_l}^z \forall n$ it is all-right, otherwise she realizes a possible attack of an outsider Eve in the quantum channel. As for measurements in \mathcal{B}_x she compares $j_{a_l}^x$ with $J_l^x = \prod_{n=1}^N j_{n_l}^x$: if $j_{a_l}^x = J_l^x$ it is all-right [22], otherwise there is Eve in the line. If the error rate exceeds a predetermined small value Alice tells Bobs to restart the whole process, otherwise they record the order of the remaining shared $|\Psi_m\rangle$ -states and can use them for the problem-giving process following the steps from a1) to a4).

The $|\Phi_m\rangle$ -sharing process

The states $\{|\Phi_m\rangle\}$ can be securely shared between the participants as follows.

- d1) Alice generates a large enough number of identical states $\{|\Psi_m\rangle\}$ [21]. She then applies on each of the identical states a unitary operator U_p determined by Eq. (5) to transform them into the $|\Phi_p\rangle$ -states defined in Eq. (4) which are nonidentical states [23]. Afterward, for each $|\Phi_p\rangle$, she keeps qubit a_p and sends qubits $1_p, 2_p, \dots, N_p$ to Bob 1, Bob 2, ..., Bob N , respectively. Before sending a qubit n_p Alice authenticates Bob n of that action.
- d2) After receiving a qubit each Bob also authenticates Alice independently.
- d3) Alice selects at random a large enough subset $\{|\Phi_l\rangle\}$ out of the shared $|\Phi_p\rangle$ -states and lets Bobs know that subset. For each state $|\Phi_l\rangle$ of the subset Alice measures her qubit randomly in either \mathcal{B}_z or \mathcal{B}_x , then asks Bobs to measure their qubits in the same basis as hers.
- d4) Alice requires each Bob to publicly reveal the outcome of each his measurement and makes a proper analysis. For those measurements in \mathcal{B}_z she verifies the equalities $j_{a_l}^z = \delta_{0,s_{n_l}} j_{n_l}^z + \delta_{1,s_{n_l}} (j_{n_l}^z \oplus 1)$. If the equalities hold for every n it is all-right, otherwise the quantum channel was attacked. As for measurements in \mathcal{B}_x she compares $j_{a_l}^x$ with $J_l^x = \prod_{n=1}^N j_{n_l}^x$: if $j_{a_l}^x = J_l^x$ it is all-right [24], otherwise the quantum channel was attacked. If the error rate exceeds a predetermined value Alice tells Bobs to restart the whole process, otherwise they record the order of the remaining shared $|\Phi_p\rangle$ -states and can use them for the solution-collecting process following the steps from b1) to b4).

Security of the entanglement-sharing process

To gain useful information about the exam, Eve must attack the quantum channel during the entanglement-sharing process. Below are several types of attack that Eve commonly uses.

Measure-Resend Attack. In \mathcal{B}_z Eve measures the qubits emerging from Alice and then resends them on to Bobs. After Eve's measurement the entangled state collapses into a product state and her attack is detectable when Alice and Bobs use \mathcal{B}_x for a security check [25].

Disturbance Attack. If Alice and Bobs check security only by measurement outcomes in \mathcal{B}_x , then Eve, though cannot gain any information, is able to make the protocol to be denial-of-service. Namely, for each n , on the way from Alice to Bob n , Eve applies on qubit n an operator $u(v_{n_m})$ as defined in Eq. (6) with v_{n_m} randomly taken as either 0 or 1, then lets the qubit go on its way. By doing so the disturbed states become truly random and totally unknown to everybody, hence no cryptography is possible at all. Though measurements in \mathcal{B}_x cannot detect this type of attack [26], those in \mathcal{B}_z can [27].

Entangle-Measure Attack. Eve may steal some information by entangling her ancilla (prepared, say, in the state $|\chi\rangle_E$) with a qubit n (assumed to be in the state $|i\rangle_n$) before the qubit reaches Bob n : $|\chi\rangle_E |i\rangle_n \rightarrow \alpha |\chi_i\rangle_E |i\rangle_n + \beta |\overline{\chi_i}\rangle_E |i \oplus 1\rangle_n$ where $|\alpha|^2 + |\beta|^2 = 1$ and ${}_E \langle \chi_i | \overline{\chi_i} \rangle_E = 0$. After Bob n measures his qubit Eve does so with her ancilla and thus can learn about the Bob's outcome. Yet, with a probability of $|\beta|^2$ Eve finds $|\overline{\chi_i}\rangle_E$ in which case she is detected if the security check by Alice and Bobs is performed in \mathcal{B}_z [28].

Intercept-Resend Attack. Eve may create her own entangled states $|\Psi'\rangle_{a'_m 1'_m \dots N'_m}$ ($|\Phi'\rangle_{a'_m 1'_m \dots N'_m} = U'_m |\Psi'\rangle_{a'_m 1'_m \dots N'_m}$ where $U'_m = I_{a'_m} \otimes u(s'_{1_m}) \otimes u(s'_{2_m}) \otimes \dots \otimes u(s'_{N_m})$ with $\{s'_{n_m}\}$ an arbitrary random string). Then she keeps qubit a'_m and sends qubit n'_m to Bob n . When Alice sends qubits n_m to Bobs Eve captures and stores all of them. Subsequently, after Alice's and Bobs' measurements, Eve also measures her qubits a'_m and the qubits n_m she has kept to learn the corresponding keys. This attack is detected as well when Alice and Bobs use \mathcal{B}_z -measurement outcomes for their security-check [29].

Masquerading Attack. Eve may pretend to be a Bob in the $|\Psi_m\rangle$ -sharing process to later obtain Alice's problem. Likewise, she may pretend to be Alice in the $|\Phi'_m\rangle$ -sharing process to later collect Bobs' solutions. Such pretenses are excluded because each Bob after receiving a qubit has to inform Alice and Alice before sending a qubit has also to inform all Bobs. The classical communication channels Alice and Bobs possess have been assumed highly authentic so that any disguise must be disclosed.

2.2. Asymptotically secure protocol

In some circumstances an urgent exam needs to be organized but no prior quantum nonlocal arrangements are available at all. We now propose a protocol to directly accomplish such an urgent task. At that aim, Alice has to have at hand a large number of states $\{|\Psi_m\rangle\}$ and $\{|\Phi_m\rangle = U_m |\Psi_m\rangle\}$. Let M (M') be length of Alice's problem (Bobs' solution) and T the time provided for Bobs to solve the problem.

The direct problem-giving process

Alice can directly give her problem to Bobs by "running" the following program.

- e1) $m = 0$.
- e2) $m = m + 1$. Alice picks up a state $|\Psi_m\rangle$, keeps qubit a_m and sends qubits $1_m, 2_m, \dots, N_m$ to Bob 1, Bob 2, ..., Bob N , respectively. Before doing so Alice informs all Bobs via her authentic classical channels.
- e3) Each Bob confirms receipt of a qubit via their authentic classical channels.
- e4) Alice switches between two operating modes: the control mode (CM) with rate c and the message mode (MM) with rate $1 - c$. Alice lets Bobs know which operating mode she chose.
 - e4.1) If CM is chosen, Alice measures qubit a_m randomly in \mathcal{B}_z or \mathcal{B}_x with an outcome $j_{a_m}^z$ or $j_{a_m}^x$, then lets Bobs know her basis choice and, asks them to measure their qubits n_m in the chosen basis. After measurements each Bob publicly publishes his outcome $j_{n_m}^z$ or $j_{n_m}^x$. Alice analyzes the outcomes: if $j_{a_m}^z = j_{1_m}^z = j_{2_m}^z = \dots = j_{N_m}^z$ or $j_{a_m}^x = \prod_{n=1}^N j_{n_m}^x$ she sets $m = m - 1$ and goes to step e2) to continue, else she tells Bobs to reinitialize from the beginning by going to step e1).
 - e4.2) If MM is chosen, Alice measures qubit a_m in \mathcal{B}_z with an outcome $j_{a_m}^z$ and publicly reveals $x_m = j_{a_m}^z \oplus q_m$. Each Bob measures his qubit also in \mathcal{B}_z with an outcome $j_{n_m}^z$, then decodes Alice's secret bit as $q_m = j_{n_m}^z \oplus x_m$. If $m < M$ Alice goes to step e2) to continue, else she publicly announces: "My problem has been transferred successfully to all of you. Please return your solution after time T ".

The direct solution-collecting process

After time T Alice can directly collect Bobs' solutions by "running" another program as follows.

- g1) $m = 0$.

- g2) $m = m + 1$. Alice picks up a $|\Phi_m\rangle$, keeps qubit a_m and sends qubits $1_m, 2_m, \dots, N_m$ to Bob 1, Bob 2, ..., Bob N , respectively. Before doing so Alice informs all Bobs via her authentic classical channels.
- g3) Each Bob confirms receipt of a qubit via their authentic classical channels.
- g4) Alice switches between two operating modes: the CM with rate c and the MM with rate $1 - c$. Alice lets Bobs know which operating mode she chose.
 - g4.1) If CM is chosen, Alice measures qubit a_m randomly in \mathcal{B}_z or \mathcal{B}_x with an outcome $j_{a_m}^z$ or $j_{a_m}^x$, then lets Bobs know her basis choice and, asks them to measure their qubits n_m in the chosen basis. After measurements each Bob publicly publishes his outcome $j_{n_m}^z$ or $j_{n_m}^x$. Alice analyzes the outcomes: if $j_{a_m}^z = \delta_{0,s_{n_m}} j_{n_m}^z + \delta_{1,s_{n_m}} (j_{n_m}^z \oplus 1)$ for every n or $j_{a_m}^x = \prod_{n=1}^N j_{n_m}^x$ she sets $m = m - 1$ and goes to step g2) to continue, else she tells Bobs to reinitialize from the beginning by going to step g1).
 - g4.2) If MM is chosen, Alice measures qubit a_m in \mathcal{B}_z with an outcome $j_{a_m}^z$ and each Bob measures his qubit also in \mathcal{B}_z with an outcome $j_{n_m}^z$. Each Bob publicly reveals $y_{nm} = r_{nm} \oplus j_{n_m}^z$ and Alice decodes Bobs' secret bits as $r_{nm} = y_{nm} \oplus [\delta_{0,s_{n_m}} j_{a_m}^z + \delta_{1,s_{n_m}} (j_{a_m}^z \oplus 1)]$ for $n = 1, 2, \dots, N$. If $m < M'$ Alice goes to step g2) to continue, else she publicly announces: "*Your solutions have been collected successfully*".

As described above, in the direct problem-giving (solution-collecting) process Alice alternatively gives (collects) secret bits and checks Eve's eavesdropping. These direct protocols also stand against the types of attack mentioned above. The protocols terminate immediately whenever Eve is detected in a control mode. However, Eve might get a partial information before her tampering is disclosed. Such an information leakage can be reduced as much as Alice wants by increasing the control mode rate c at the expense of reducing the information transmission rate $r = 1 - c$. For short strings Q and R_n (see Eq. (1) and Eq. (2)) Eve's detection probability may be quite small. But, the longer the strings the higher the detection probability. In the long-string limit the detection probability approaches one, i.e. Eve is inevitably detected. In this sense, the direct quantum exam protocols are asymptotically secure only.

3. Conclusion

We have proposed two protocols for organizing a quantum exam [30] basing on a judicious use of appropriate multipartite entangled states. The first protocol is absolutely secure iff the participants have successfully shared the necessary entanglement in advance. We also provide methods for sharing the multipartite entanglement in the presence of a potential eavesdropping outsider. The second protocol can be processed directly without a prior entanglement sharing. This advantage is however compromised by a lower confidentiality level or by a slower information transmission rate. Both the protocols have been shown to sustain various kinds of attacks such as measure-resend attack, disturbance attack, entangle-measure attack, intercept-resend attack and masquerading attack. Our protocols work well in an idealized situation with perfect entanglement sources/measuring devices and in noiseless quantum channels which we have assumed for simplicity. We are planning to further develop our protocols to cope with more realistic situations.

Acknowledgments.

The author is grateful to Professor Hai-Woong Lee from KAIST for useful discussion and comments. This research was supported by a Grant (TRQCQ) from the Ministry of Science and Technology of Korea and also by a KIAS R&D Fund No 6G014904.

-
- [1] E. Schrödinger, Naturwiss. 23 (1935) 807.
 - [2] D.M. Greenberger, M.A. Horne, A. Zeilinger, in: M. Kafatos (Ed.), Bell's Theorem, Quantum Theory and Conceptions of the Universe, Kluwer, Dordrecht, 1989, p.69; H.J. Bernstein, Foundation Phys. 29 (1999) 521.
 - [3] R. Jozsa, N. Linden, quant-ph/0201143.
 - [4] A.J. Scott, Phys. Rev. A 69 (2004) 052330.
 - [5] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000, p. 513.
 - [6] S. Sachdev, Quantum Phase Transitions, Cambridge University Press, Cambridge, U.K., 2000; A. Anfosso, P. Giorda, A. Montorsi, F. Traversa, Phys. Rev. Lett. 95 (2005) 056402.
 - [7] V. Vedral, New J. Phys. 6 (2004) 22.

- [8] A. Karlsson, M. Bourennane, Phys. Rev. A 58 (1998) 4394;
P. van Loock, S.L. Braunstein, Phys. Rev. Lett. 84 (2000) 3482;
P. van Loock, S.L. Braunstein, Phys. Rev. Lett. 87 (2001) 247901;
V.N. Gorbachev, A.I. Trubilko, A.I. Zhibila, J. Opt. B: Quantum Semiclss. 3 (2001) S25;
Nguyen Ba An, Phys. Rev. A 68 (2003) 022321.
- [9] J. Kempe, Phys. Rev. A 60 (1999) 910;
G. A. Durkin, C. Simon, D. Bouwmeester, Phys. Rev. Lett. 88 (2004) 187902.
- [10] R. Cleve, D. Gottesman, H.-K. Lo, Phys. Rev. Lett. 83 (1999), 648;
M. Hillery, V. Buzek, A. Berthiaume, Phys. Rev. A 59 (1999) 1829.
- [11] A.K. Pati, Pramana-J. Phys. 59 (2002) 217;
Nguyen Ba An, Phys. Rev. A 69 (2004) 022315.
- [12] D. Bruss, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, J. A. Smolin, Phys. Rev. A 57 (1998) 2368;
M. Murao, D. Jonathan, M. B. Plenio, V. Vedral, Phys. Rev. A 59 (1999) 156;
C.-W. Zhang, C.-F. Li, Z.-Y. Wang, G.-C. Guo, Phys. Rev. A 62 (2000) 042302.
- [13] M. Fitzi, N. Gisin, U. Maurer, Phys. Rev. Lett. 87 (2001) 217901.
- [14] J. Preskill, J. Mod. Opt. 47 (2000) 127.
- [15] W. Dur, G. Vidal, J.I. Cirac, Phys. Rev. A 62 (2000) 062314.
- [16] G. Adesso, A. Serafini, F. Illuminati, Phys. Rev. Lett. 93 (2004) 220405;
C. S. Yu, H. S. Song, Phys. Rev. A 71 (2005) 042331.
- [17] X. Wang, B.C. Sanders, Phys. Rev. A 65 (2002) 012303;
M. Eibl, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Zukowski, H. Weinfurter, Phys. Rev. Lett. 90 (2003) 200403;
Nguyen Ba An, J. Kim, quant-ph/0303149;
H. Mikami, Y. Li, T. Kobayashi, Phys. Rev. 70 (2004) 052308;
A. Olaya-Castro, N.F. Johnson, L. Quiroga, Phys. Rev. A 70 (2004) 020301(R);
P.B. Stiffell, M.J. Everitt, T.D. Clark, C.J. Harland, J.F. Ralph, Phys. Rev. B 72 (2005) 014508;
A. Olaya-Castro, N.F. Johnson, L. Quiroga, Phys. Rev. Lett. 94 (2005) 110502;
Nguyen Ba An, Phys. Lett. A 344 (2005) 77;
W. Dur, J. Calsamiglia, H.J. Briegel, Phys. Rev. A 71 (2005) 042336.
- [18] A.C. Doherty, P.A. Parrilo, F.M. Spedalieri, Phys. Rev. A 71 (2005) 032333;
G. Tóth, O. Gühne, Phys. Rev. Lett. 94 (2005) 060501.
- [19] Nguyen Ba An, Phys. Lett. A 328 (2004) 6;
Nguyen Ba An, J. Kor. Phys. Soc. (2005) in print.
- [20] S.S. Jang, H.W. Lee, Phys. Lett. A 339 (2005) 430.
- [21] A state $|\Psi_m\rangle \equiv |\Psi\rangle_{a_m 1_m \dots N_m}$ can be generated from the product state $|00\dots 0\rangle_{a_m 1_m \dots N_m}$ as $|\Psi\rangle_{a_m 1_m \dots N_m} = CNOT_{a_m N_m} \otimes \dots \otimes CNOT_{a_m 2_m} \otimes CNOT_{a_m 1_m} \otimes H_{a_m} |00\dots 0\rangle_{a_m 1_m \dots N_m}$, where $CNOT_{xy}$ is a control-NOT gate with x (y) being the control (target) qubit and H_x is the Hadamard gate acting on qubit x .
- [22] This checking strategy comes out from the fact that a state $|\Psi\rangle_{a_l 1_l \dots N_l}$ always has a positive parity, i.e. $j_{a_l}^x \prod_{n=1}^N j_{n_l}^x = +1$ definitely.
- [23] Since each U_p is managed by Alice alone, she is the only one who knows the parameters $s_{1_p}, s_{2_p}, \dots, s_{N_p}$ though each of them is randomly chosen between 0 and 1. That is, only Alice is able to distinguish states $|\Phi_p\rangle$ with certainty.
- [24] This checking strategy comes out from the fact that a state $|\Phi\rangle_{a_l 1_l \dots N_l}$ also has definitely a positive parity.
- [25] This is because any product state $|i_a i_1 i_2 \dots i_N\rangle_{a_l 1_l \dots N_l}$ with $i_a, i_n \in \{0, 1\}$, when measured in \mathcal{B}_x , yields either “plus” or “minus” parity with an equal probability.
- [26] Because any entangled state $(|i_a i_1 i_2 \dots i_N\rangle_{a_l 1_l \dots N_l} + |\bar{i}_a \bar{i}_1 \bar{i}_2 \dots \bar{i}_N\rangle_{a_l 1_l \dots N_l}) / \sqrt{2}$, with \bar{i} the negation of $i = \{0, 1\}$, has definitely a positive parity.
- [27] Because $v_{n_m} \neq s_{n_m}$ in general.
- [28] Because in this case what Bob actually finds is $|i \oplus 1\rangle_n$ instead of the should-be $|i\rangle_n$.
- [29] Because there are no correlations at all between qubit a_m and qubits n'_m .
- [30] If one likes, the name “quantum exam” can alternatively be replaced by “quantum multiparty interview” (or “quantum ballot”) for which Alice plays the role of the interviewer (or the selection committee chair) and Bobs play the role of interviewees (or balloters).